Following the rules is not enough

The EU is reshaping the regulatory landscape, but smart companies will do more, say Brunswick's PETER LINDELL and ANNALISA BARBAGALLO

In 1995, a tiny company called Cadabra, deciding its name sounded too much like "cadaver," settled on a new one: Amazon. It sold books online and filled orders out of a garage. That was the same year the European Union adopted the Data Protection Directive that regulated personal data privacy.

While Amazon went from garage-based startup to a market capitalization of more than $300 billion, the directive was not as successful. Its principles were interpreted and enforced differently across the EU, and they were also challenged by profound changes in technology and the explosive global development of companies such as Amazon.

Two new pieces of legislation, the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS Directive), are poised to modernize and standardize Europe's laws on data privacy and cybersecurity. Their reach could even extend beyond European borders, and potentially apply to companies outside Europe whose customers include EU citizens.

These laws will affect the way companies collect and protect consumer data, and change the extent to which European governments can regulate – and punish – businesses. Companies breaking these rules will face fines as costly as 4 percent of their global revenue or €20 million ($22 million), whichever is greater.

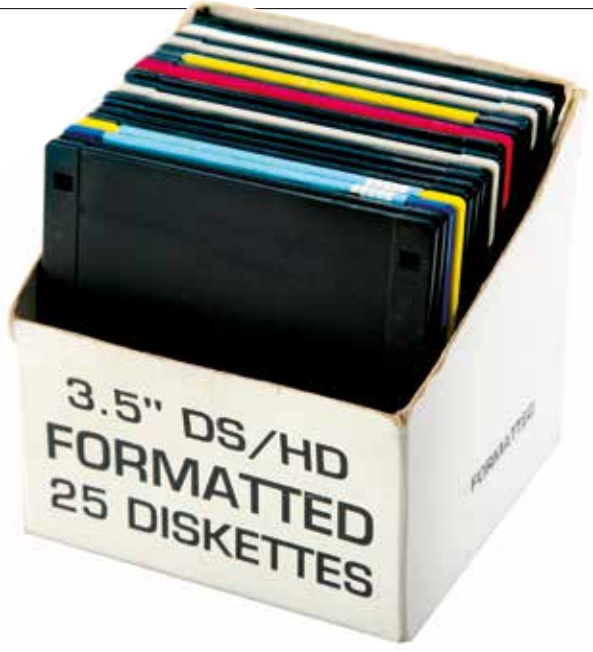
While the new regulations are significant for their scope and severity, they point in a direction where many companies are already headed. As these organizations have realized, there is no need to wait for regulations to create robust cybersecurity policies or to be transparent with customers about how their data is being used and protected.

THE FIRST PIECE OF LEGISLATION, the GDPR, is set to become law across the EU in 2018. When it does, it will give EU citizens greater control and visibility of their data held by third parties.

Consumers will have to give consent for companies to collect their data and this consent must be tied to a specific service or product. Clear wording will be required; no more lengthy, indecipherable agreements.

The GDPR will also require that within 72 hours of a data breach that could jeopardize "the rights and freedoms" of its customers, companies will be required to inform both regulators and those whose data may have been compromised.

5. THE FLOPPY DISK (DATA GOES PORTABLE)



First sold in 1971, the floppy disk transformed data sharing. The earliest floppies were a cumbersome 8x8 inches, but suddenly data was portable, accessible – and easy to steal. Smaller sizes followed. Most were replaced by CDs and, later, USB flash drives – but not all. A report by the US Government Accountability Office recently revealed that the Department of Defense was still using 8-inch floppy disks to "coordinate the operational functions of the United States' nuclear forces." This veteran technology is scheduled to be retired by the end of 2017.

PHOTOGRAPH: MIKE LEDRAY, SHUTTERSTOCK

Customers will also have a "right to be forgotten," allowing them to ask companies to delete data. This aspect of the law has already been applied in some individual cases and supported by a ruling of the European Court of Justice.

THE SECOND piece of legislation, the NIS Directive, has not yet been passed by the European Parliament but is expected to be approved. This directive places stricter security requirements on all companies based in the EU, and mandates that companies in critical sectors, such as energy, finance and healthcare, inform government regulators of significant disruptions and breaches. In what some have seen as a controversial move, the list of critical sectors has been expanded to include technology companies such as Cisco, Google and Amazon.

While these laws are both expected to come into force in two years, it remains to be seen how they will be interpreted and enforced, and the extent to which they will be challenged in court.

However, four things are clear. First, companies must be fluent in the new regulations and ensure compliance. Armed with popular support and public funding, it is safe to assume regulators will actively police and enforce the new laws. Consumers and the media are also tuned in and, along with regulators, will be asking new questions. Breaches are likely to be expensive and highly visible, especially given the new disclosure requirements. The reputational cost will almost certainly be greater than any direct fines.

Second, given their importance, these regulations should not be thought of as solely an IT issue, a compliance issue, or even just a public affairs issue, though the new laws will have repercussions on all three. In the C-suite and boardroom, this is a business-critical issue that leaders should be thinking about and planning for. What steps are in place to ensure employees are learning about and complying with the latest regulations? Who will communicate with regulators? What does it mean for your business if regulators bring formal charges?

Third, training is paramount. Every employee with access to the company's network poses a risk against which even the most advanced security system cannot guard. Creating a healthy company culture is the best route to security and compliance, and that requires more than handing out copies of the latest regulations. (See "Nailing security," Page 24, for an example of a creative approach.)

Finally, while technology and the regulatory landscape have changed, the principles of good business have not. That means considering the needs of all stakeholders. Companies able to collect and monetize data have a distinct competitive advantage. The more credible a company is at explaining the purpose and benefit of the data it collects, the greater this advantage can be.

A strategy to avoid fines and escape punishment is not enough. Instead, companies need to find ways to use cybersecurity and data collection to separate themselves from the competition.

> "While technology and the regulatory landscape have changed, the principles of good business have not"

PETER LINDELL is a Partner in Brunswick's Stockholm office and part of the Cybersecurity and Privacy practice. He also advises on M&A, crisis and corporate communications. **ANNALISA BARBAGALLO** is a Partner in Brunswick's Brussels office and advises in the digital and financial services sectors.

6. TYPEWRITERS (PULLING THE PLUG)

Some have suggested that the best way to make a computer secure is to unplug it. In the wake of embarrassing and even dangerous leaks, some governments have explored that strategy. In 2012, Russia's Federal Protective Service, a government body tasked with security, spent 486,540 rubles ($15,000) buying 20 typewriters to help prevent leaks of important documents. In a 2014 interview, a member of the German government said it was considering similar measures. As fans of Cold War spy novels can attest, typewriters do not prevent data being stolen, but filing cabinets full of papers can't be compromised with a single mouse click.

IMAGE: RÜSTEM GÜRLER, GETTY